JCA-NET セミナー　2022 年 10 月 22 日

グローバル暗号化デー参加企画——暗号をライフスタイルに

暗号をライフスタイルに

強力な暗号化は、私たちがオンラインでもオフラインでも安全であり続けるための基本的な要素です。誰もメッセージを盗み聞きしたり、改ざんしたりしないという確信のもと、人々は安全に他者とコミュニケーションをとることができるのです。

にもかかわらず、世界中の政府はエンド・ツー・エンド暗号化（ E2EE ）に対する攻撃を強化しています。政府は、 E2EE を法執行機関の障害とみなしているのです。しかし、人々のデジタル・セーフティを組織的に弱体化させることは、解決策にはなりません。

エンドツーエンドの暗号化は、日常生活のオンライン化が進む世界において、セキュリティのゴールドスタンダードです。私たちは、 E2EE を弱体化させようとする政府の取り組みに反撃する必要があります。

グローバル暗号化デーには、エンドツーエンド暗号化を保護し、それを弱体化させるいかなる提案も打ち負かすための私たちの取り組みに参加するよう、皆さんに求めています。私たちはすでに、エンドツーエンド暗号化にバックドアを設けようとする試みがいかに支持されないかを示しました。今、私たちは、各国政府が提案するその他の抜け道を阻止する必要があります。

暗号をライフスタイルに

暗号は、インターネットなどコンピューター通信では必須の仕組みになっています。ネットバンキングやクレジット決済などはわかりやすい例です。ウエッブを閲覧するときなども URL が従来の「http」から「https」へと変更されているサイトが増えていますが、これも、自分のパソコンなどからサイトにアクセスする経路上で第三者による「盗聴」や改竄を防止する暗号化の仕組みです。

他方で、最も日常的に用いられているメールや、パソコンに保存されているデータなどは暗号化されないままになっている場合がまだ一般的です。これらについては、ユーザーが自覚的に「暗号化」の仕組みを導入することが課題になっています。

他方で、各国政府は、企業や政府のセキュリティにおいては暗号化を尊重する一方で、犯罪捜査やテロ対策などの名目では、政府が解読できない暗号化を規制しようとする動きや、通信事業者を巻き込んでの暗号の弱体化の動きも活発です。

大切な機密文書だけを暗号化するよりもむしろ、日常的に可能なかぎり全てのコミュニケーションやデータを暗号化する方が、大切な文書の保護をより確実にします。この意味で、ネットやコンピューターを暗号化を当たり前のものとして使えるようにすることが大切なのです。

暗号をライフスタイルに

わたしたちが使うコンピュータやスマホはコミュニケーションの道具です。

コミュニケーションとは、私とあなた、私と誰かとの間の「対話」

対話は

- よく知っている「あなた」との対話
- あまりよく知らない「あなた」との対話
- 人間ではなく、ネット上の「ウエッブサイト」との「対話」

など様々

暗号をライフスタイルに

(続)わたしたちが使うコンピュータやスマホはコミュニケーションの道具です。

コミュニケーションの「流儀」は、相手によって変わります。

- 仲のよいひとたちとの対話
- 他人には知られたくない相手との対話
- 仕事などでの対話
- あまりよく知らない人との対話
- 仲のよくない人たちとの対話
- 対立や喧嘩している人たちとの対話

どのような場合であれ、同じコミュニケーションの道具を使う。

暗号をライフスタイルに

(続)わたしたちが使うコンピュータやスマホはコミュニケーションの道具です。

コミュニケーションの「流儀」は、相手によって変わります。

- 仲のよいひとたちとの対話→仲良し以外には漏れないように
- 他人には知られたくない相手との対話→誰にも内緒
- 仕事などでの対話→守秘義務！
- あまりよく知らない人との対話→とりあえず警戒
- 仲のよくない人たちとの対話→弱味を握られたくない
- 対立や喧嘩している人たちとの対話→相手の弱味を知りたい

どのような場合であれ、同じコミュニケーションの道具を使う。

暗号をライフスタイルに

コンピュータを介さない昔には、人間は、自分の話すこと、書くことに注意することで、コミュニケーションのリスクのほとんどすべてに対処することができた。

「話すこと、書くことに注意する」とは、

- リスクを自覚・実感できるか、あるいはイメージ可能である
- リスクを回避するための方法を知っている
- コミュニケーションのリスクは経験として蓄積され、継承される

コンピュータ・コミュニケーション上の「不安全」（リスク）では上記の対処方法が適用できないことがほとんど。

暗号をライフスタイルに

たとえば、親友に手紙を書く。

「これは君だけに教えるのだけれどもね....」

この手紙のリスクは

- 親友が誰かに内容を漏らす
- 親友が不注意に手紙を放置して誰かに読まれる
- ポストから盗まれる
- 郵便局が密かに開封して内容を読む

これは「実感」できるリスクなので、「私」はリスクを覚悟して、書く内容を工夫するか、書くのをやめて直接口頭で相手に話すことで証拠を残さないようにするか、経験や実感から判断できる回避策を工夫する。たぶん、これがネットを介したメールでもリスク感覚の基準になっているかもしれないが....

暗号をライフスタイルに

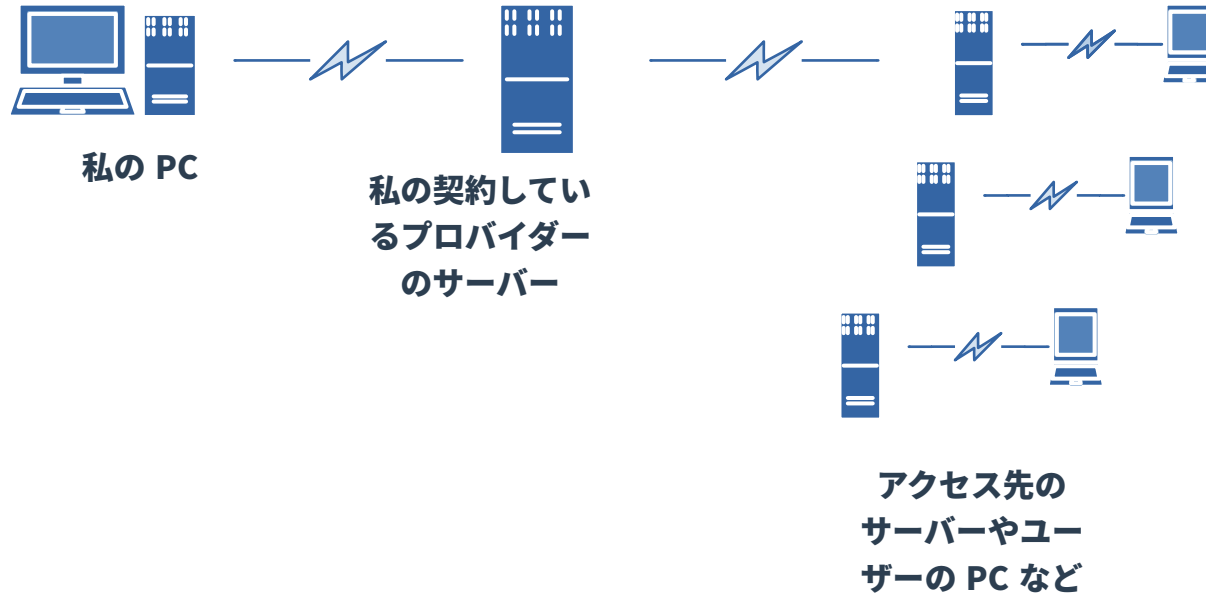
コンピュータ・コミュニケーションの安全で念頭に置くべきことは、

コミュニケーションの「不安全」（リスク）を実感できるとは限らない

すでに被害を被っていても、気づかないことが多い

私と誰かのコミュニケーションは、郵便とは違い多くの実感しがたい仕組みによって成り立っている。

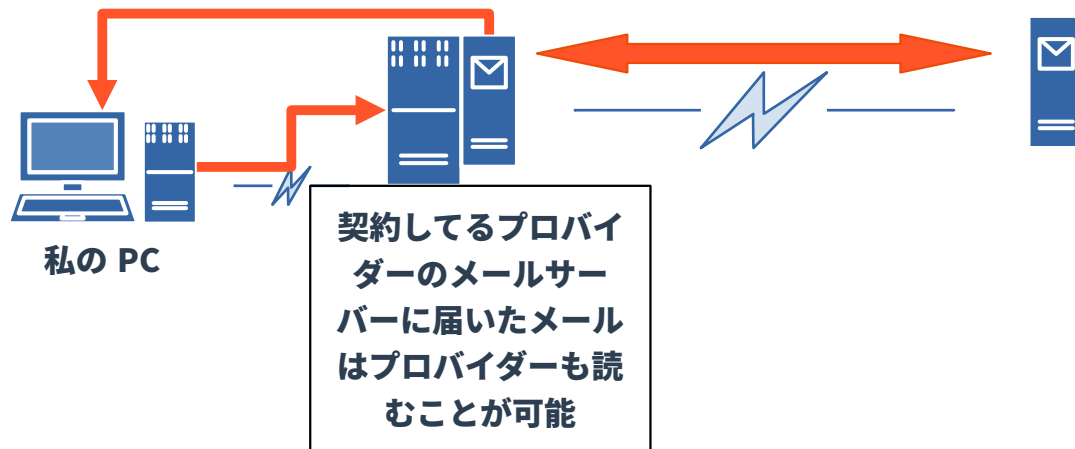
暗号をライフスタイルに

ネットの仕組みのなかで、私が実感できるものは全体のなかのごく僅かな部分だけだ。

コミュニケーションに関連するのは、

- 自分のパソコン
- プロバイダーのサーバー
- ネットワークの経路
- 接続先のコンピュータ

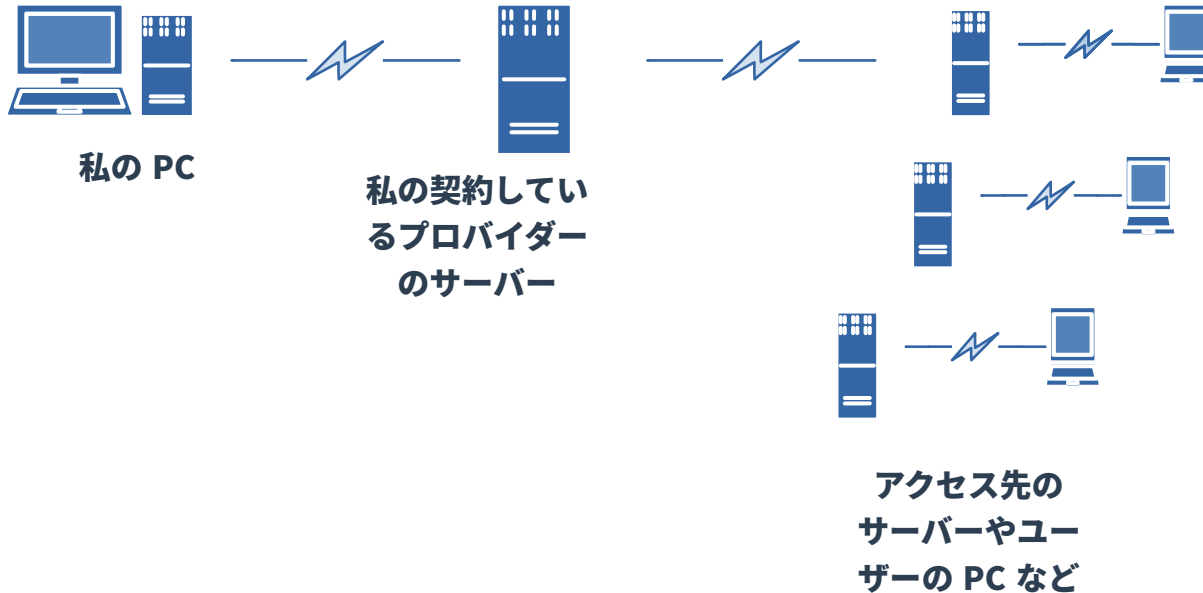
このいずれも、どのような仕組みなのかは実感できないし、理解することも難しい。

暗号の導入について

通常のメール サービスの場合

「メールは、サーバーを介して送受信が行われます。自分から相手へメールを送信する場合、メールソフトでメールを作成して送信すると、まず自社のメールサーバーに送られます。そして、自社のメールサーバーが宛先のメールアドレスを確認し、相手先のメールサーバーへメールを送り、相手のメールソフトに受信の知らせが行くという仕組みです。

この一連の流れの中で、自分が送信して相手が受信するまでの間に情報が漏えいするリスクが潜んでいます。」（Softbank ）

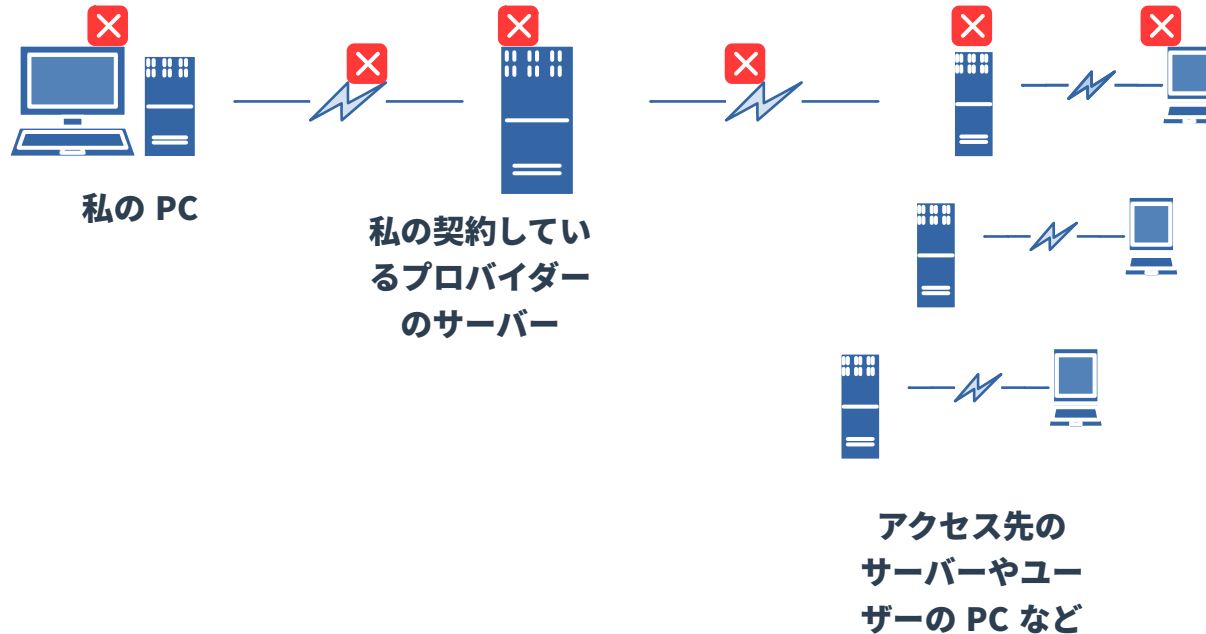
暗号の導入について

ネットの仕組みのどこにリスクがあるのかを実感できるとは限らない。

コミュニケーションのリスクに関連するのは、

- 自分のパソコン
- プロバイダーのサーバー
- ネットワークの経路
- 接続先のコンピュータ

このいずれも、**どのようなリスクがあるのかは実感することも、理解することも難しい。**

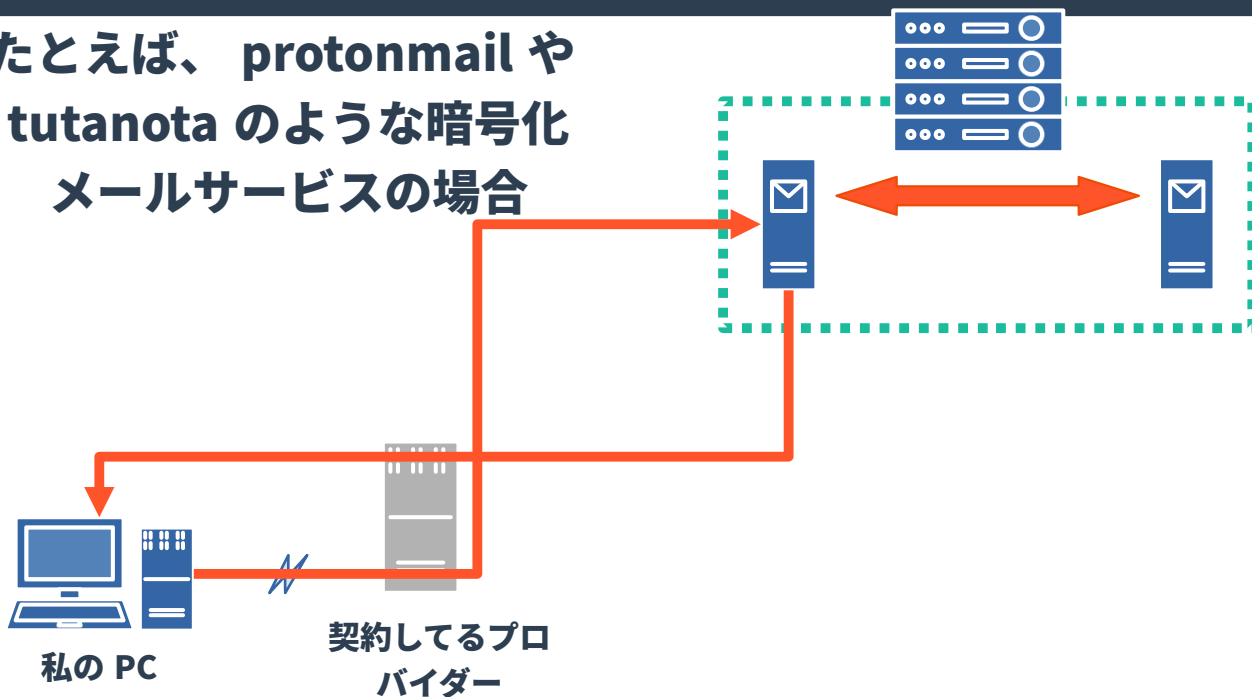
暗号の導入について

コミュニケーションを意図しない第三者に覗かれないようにすること

漏洩のリスクとして

- ネット回線の盗聴 (違法、合法)
- プロバイダーからの過失での漏洩
- プロバイダーなどからの「適法」なデータの提供

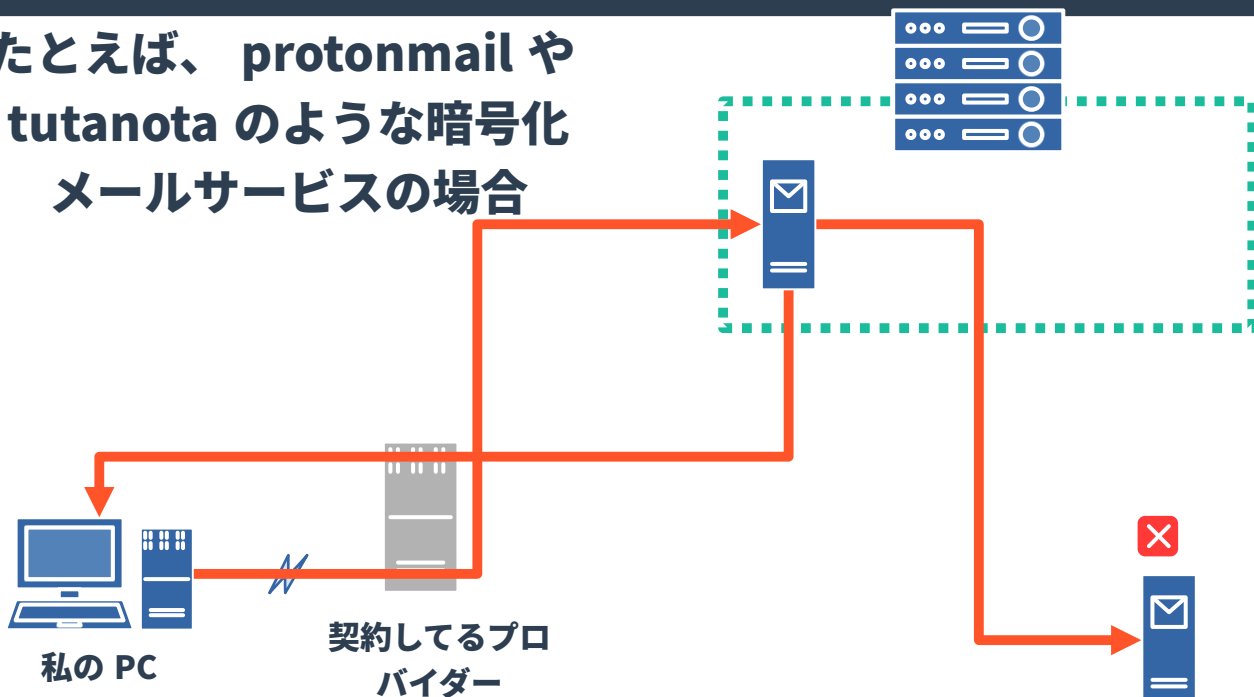
など

私と通信相手だけが理解できるようにメッセージを暗号化する

暗号の導入について

proton や tutanota では暗号化されたままデータが保管され、通信相手が同じサービスを使っていれば復号されることなく相手に送信される。

- サービスを提供する企業もデータの内容を把握できない。
- 自分が契約しているプロバイダー (OCN とか au とか) もメールの内容を把握できない。

私の PC にもプロバイダーのサーバーにもメールのデータは存在しない。画面上では、データがあたかも自分の PC にあるかのように錯覚してしまうかもしれないが。

暗号の導入について

暗号化メールサービスの限界

proton や tutanota では暗号化されたままデータが保管されるが、通信相手が別のサービスを使っていれば、**相手の、メールサーバーでは平文で保存されるので盗聴のリスクがある。**
しかし、**相手からの受信メールは暗号化されてメールサーバーに保管される。**

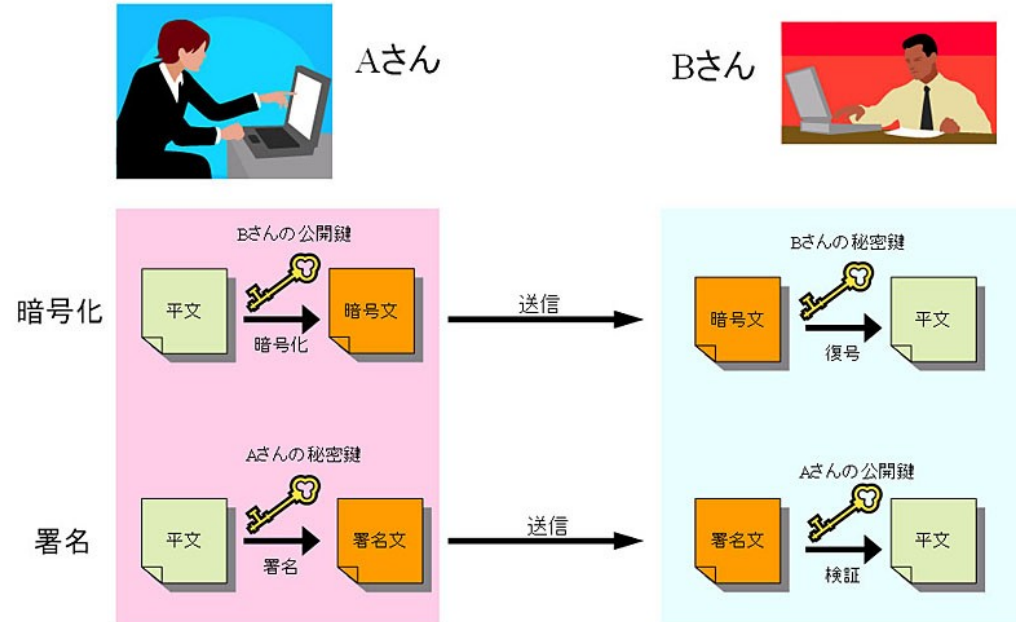
暗号の導入について

誰とでも暗号化メールのやりとりが可能になるためにはどうしたらいいのか

公開鍵暗号方式

- **メッセージの暗号化**
- **メッセージの信憑性**

この仕組みを使うためには
「鍵」を作成する
公開鍵暗号をサポートしているメールソフト (Thunderbird など) を使う

ITメディアエンタープライズ：PGP？ S/MIME？ 電子署名の違いを学ぶ

暗号の導入について

Linux-info のメーリングリストに 10 月初めころに右のようなメールを送信して、何人かの方から問い合わせがありました。

このメールは、公開鍵暗号の仕組みをつかって「署名」したものです。

これは、メールが本当に本人からのものかどうかを確認できる仕組みになります。確認方法はちょっと面倒かもしれません。
解説例：国税庁
「PGP 署名 確認方法」などで検索してみてください

[Linux-info 980] firefoxでJitsi-meetを使う場合の注意

発信者 toshimaru ogura (Linux-info 経由) <linux-info@list.jca.apc.org> 日付 2022-10-01 16:35

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
```

小倉です。先日のセミナーで、jitsi-meetをforefoxで使う場合についての質問がありました。いくつか注意点があります。画面共有の方法がChrome系とはちょっと違うところがあること、正式のサポートがfirefox ESR版であることなどを下記に記載しました。あまりうまく説明できていないかもしれません。またfirefoxのESR版への移行方法についても参照すべきサイトへのリンクを紹介しているだけで具体的な方法を書けていません。

https://www.jca.apc.org/jca-net/sites/default/files/2022-10/firefox20221001.pdf

参照していただいて、質問などあれば、よろしく。小倉

toshimaru ogura
rumatoshi@protonmail.com

-----BEGIN PGP SIGNATURE-----
Version: ProtonMail

wsFzBAEBCAAGBQJjN+2nACEJELRcjz3ijsoPFiEEqHXMqIoseIESbOmrtFyP
PeKOyg/irQ//S4SimmnIS6WfqceC+A7BHC10ezF/3TgbvbwLcY8sjfomEaSA
0Z3QdplA/kwk8hKoS5knbNR/h2bPkyNSTVq5zzCgC/BV/6/7w/YMDMdx+5Kw
7fJXGGyhL69Iv8TUOxuq/fqXQ5PyjoK7CfhGWSgF28eY3Ggq1CCVUClRoDoG
qq7a2/6kcEHoHZvxQoK9U15wcBy+XNYF8cub3BHFIlRdUySBrbG+TFvjjyxl
t5tPALife85CPtc37caw3XVWZx7/h9zvVtbnmMXmP7fFJgueLMiOKOX5mpDq
GlFBD+Fzdl54NoyixiBqYg48/6IIdWrW2XBRlKDYkZJW0wTDSUUd3WVV1aOB
D/2P0ULSEV10S21c03rVs9aAHmYopkB5MGpYlNS0rtzwIpP4Bpe19whs0CHD
1CE6LgDVUnEmFeRIY16FLTJf+c+j5PI4xDf/6JlOTbQSXA6gpRo4NAn3Jg21
+jwc2f7ZXWQiuX4hnQUaB+yRI/aQKrJw+tZLSTuWAeKP2LafVqqrQe1sDTKL
8hHVAv9z0x45AJh088MXB1H4oyObpwFKioEjCz7TUhCnsx++6LifgxsnTDJK
UUhJSz9PStgAFuE2NxopvBjt4fUZ3ZemzCrZ3zeSSKg4NxhJczxQhaZnAniR
NzN0BU9umKuGOg5knpRuxc58ZINzVZ2FP5g=
=mrkR
-----END PGP SIGNATURE-----

暗号の導入について

右の例は、 Debian という Linux OS のディストリビューションが配信しているセキュリティ関連情報 (10 月 19 日付) です。内容の改竄の有無を確認できるように公開鍵暗号を使って署名しています。

[SECURITY] [DSA 5259-1] firefox-esr security update

発信者 Moritz Muehlenhoff <jmm@debian.org> 日付 木 04:37

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

- -------------------------------------------------------------------------
Debian Security Advisory DSA-5259-1                   security@debian.org
https://www.debian.org/security/                     Moritz Muehlenhoff
October 19, 2022                      https://www.debian.org/security/faq
- -------------------------------------------------------------------------

Package        : firefox-esr
CVE ID         : CVE-2022-42927 CVE-2022-42928 CVE-2022-42929 CVE-2022-42932

Multiple security issues have been found in the Mozilla Firefox
web browser, which could potentially result in the execution
of arbitrary code or information disclosure.

For the stable distribution (bullseye), these problems have been fixed in
version 102.4.0esr-1~deb11u1.

We recommend that you upgrade your firefox-esr packages.

For the detailed security status of firefox-esr please refer to
its security tracker page at:
https://security-tracker.debian.org/tracker/firefox-esr

Further information about Debian Security Advisories, how to apply
these updates to your system and frequently asked questions can be
found at: https://www.debian.org/security/

Mailing list: debian-security-announce@lists.debian.org
-----BEGIN PGP SIGNATURE-----
```


iQIzBAEBCgAdFiEEtuYvPRKsOElcDakFEMKTtsN8TjYFAmNQTwwACgkQEMKTtsN8
TjbP1hAAje3LJ3LCkhXmj9JYwi5jEMADKGP5EvaSenR9Tn8i+dqJLzS6Vw00zUeP
zoZEZaEx1jQs0o9xHsWjy08YPU7vtpthp1Q8YHgIorsY41aw7pdlBoHMnXu1JaKY
4f/cCNJuUiwYtHGqT8KI6/9MMKb9oUSOTGrzClBpRE5K2FH+reYSsQfbELdCWJlp
MhVIk6gV6PpReOTd9BFlyqwkdrh7T7tUmGQMMeAG1Q4xSuBtqH5cNapMe/m60BTC
OsSmWW5tH50UB0b2VL15JRBXNw6jzPiydyaADQHJHPXQTqfnNyv8BM0waRpLW/4D
mzB+sSdn4089HbyVtfx1QlLa8EmW/f5+Zu6xCn7z6QZT5aPRrTEPk2Fcl9v2hOAb
yUNY7atms0rNvrPUkA6dDDKoSUHQ4L60FiUZJgKQAlqevg+cnXNpbvL0Koewb677
lxFvO/GZL74wClpcvsQqcYI4cXTW5TwYYwoZc29ytJ+seDaK+24YQk3XxdvWWI7w
pTOcdYvRJRNqujbzK4HlNyILqGflw3Mvgm0LqP95oyO1aHCZ1JL/cRjUXDBHbB+u
tfL8w4vUfuzdp5exawolvb5VF/V11otC4+uX2w9t4ez/31cLjKM4X5cD1E03vyUH
ik20Oin1VGTBmrYTgXcyZB7v86lPo/0q+TJwvwaIA2QLabhqatM=
=l2ad


```
-----END PGP SIGNATURE-----
```

暗号の導入について

右は JPCERT コーディネーションセンター (JPCERT/CC) が毎週発行しているニュースです。ソフトウェアの脆弱性などの情報が提供されています。ここでも内容の改竄がないかどうか確認できるように公開鍵暗号が使われています。

公開鍵は下記で公表されています。

https://www.jpcert.or.jp/jpcert-pgp.html

```
To: announce@jpcert.or.jp
Date: Wed, 19 Oct 2022 09:11:16 +0900 (JST)
Reply-To: ew-info@jpcert.or.jp

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

                                        JPCERT-WR-2022-4101
                                                  JPCERT/CC
                                                 2022-10-19

          <<< JPCERT/CC WEEKLY REPORT 2022-10-19 >>>

-------------------------------------------------------------------
■10/09(日)～10/15(土) のセキュリティ関連情報
-------------------------------------------------------------------

== 目  次 =========================================================

【1】複数のマイクロソフト製品に脆弱性
【2】複数のFortinet製品に認証バイパスの脆弱性
【3】複数のアドビ製品に脆弱性

以上。

----------
```


```
-----BEGIN PGP SIGNATURE-----

iQIcBAEBCAAGBQJjTzdFAAoJEDoQgdvpn3qqvfUP/2Zu1rbPc1e+rCdE5hPUgcam
KYkvDGtEo+1XKV43n7iPtZ4Ot1MUlb3XfLC3N615/FkRGPuXv0o3DakrjpF5g0Pv
zRvEbDTiwYJdl9RhYkjfLNh5F4Tfmq/1fwlkGZS7cB0LRBn89t6fri3Lg0QWz1nL
dusxLAv9ydDRuKSKOvH0qAzkxqzGfCYOPPuiQ15RJPWZhZIGz01aIBq55v3zG9ZO
n/xyPVVRoO8ZAxIJrJ7TZmjROYfmoTnaWqWW63Ba7DToBnO6TpibbIey37aGgr+l
zBHS621YRteliDzJC/b/HrNmywUJ67OWShEcnZf+ao2DefHnr5dqMmPBt6HKwaaI
ok1Q+O1aPJmItXNyS1RA41T4QIKJBpASsrnS/soX0B8Kp1KFC9eIzeGAIcr2TDgD
1DezscsgL8YU+EtZtVydH0jO3RG/G4QIEVloZmmWBJpo+DRA9k4T7utXEWpoOV4s
AoT1j31GaSNoVCsXzrnsFmpB20wwlfV0ApV+K1C5LGQcp7nFOMIMdNS3R0U/V44p
jiDAI3xgdWrQXacOFWeQWd1cj9Q/XHCsHaMatCyRMUtkH4cjQgzjquyPkE4CfZ1M
sxy6BCF+wqJp2kadjH6hFdNb/j5/JKDJIA2ySJ0H34aEh+x7CQKcw81q3Z4delJT
/qsde+ujUhwLERv0hCah
=5VeL
-----END PGP SIGNATURE-----
```


[End of message]

暗号の導入について

- これまでセミナーで取り上げた方法
  - Proton mail や Tutanota など暗号化メールサービスを利用する
  - ファイルの暗号化ソフト (Veracrypt)
  - ハードディスクを丸ごと暗号化する (Linux OS)
  - 公開鍵暗号 (GnuPG など)

コミュニケーションのリスクは実感しづらいので、暗号化も直感的には必要と感じられません。自覚症状のない病気のリスクと似ているかもしれません。

いかがでしたか？
できるところから「暗号」の
導入に挑戦してみませんか？